



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/791,415	03/02/2004	Santosh P. Gaur	RPS920020015US1	5405
25299 7590 10/19/2007 IBM CORPORATION PO BOX 12195 DEPT YXSA, BLDG 002 RESEARCH TRIANGLE PARK, NC 27709			EXAMINER ABRISHAMKAR, KAVEH	
			ART UNIT 2131	PAPER NUMBER
			MAIL DATE 10/19/2007	DELIVERY MODE PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

## Office Action Summary

Application No.

10/791,415

Applicant(s)

GAUR ET AL.

Examiner

Kaveh Abrishamkar

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 02 March 2004.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-29 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-29 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |   |   |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)  | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date <u>10/04/2004</u> . | 6) <input type="checkbox"/> Other: _____  |

### **DETAILED ACTION**

1. This action is in response to the communication filed on March 2, 2004. Claims 1-29 were originally received for consideration. No preliminary amendments regarding the claims were received.
2. Claims 1-29 are currently pending consideration.

### ***Information Disclosure Statement***

3. An initialed and dated copy of the Applicant's IDS form 1449, received on 10/04/2004, is attached to this Office action.

### ***Specification***

4. The disclosure is objected to because of the following informalities: In paragraph 1, the co-pending application numbers are left blank and should be filled in with the appropriate application numbers. Appropriate correction is required.

### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

Art Unit: 2131

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-2, 6-14, 17-23, and 26-29 are rejected under 35 U.S.C. 102(e) as being anticipated by Blaker et al. (U.S. Patent Publication No. US 2003/0081600 A1).

Regarding claim 1, Blaker discloses:

A system for performing security operations on network data, the system comprising:

memory (paragraph.0059, lines 1-3: "output buffer");

a data coprocessor configured to transfer data into and out of the memory (paragraph 0042, lines 1-7: *crypto-input demux and crypto-output demux*);

a plurality of processors coupled to the memory and to the data coprocessor, each processor being configured to perform, in parallel to one another, security operations on a portion of the data (paragraph 0037, lines 12-23, paragraph 45, lines 5-7: *plurality of cryptographic processors in parallel*); and

a plurality of security coprocessors coupled to the memory (paragraph 0037, lines 12-23) each security coprocessor being coupled to a respective one of the processors (Figure 1, paragraph 0037, lines 14-20: wherein the processors are coupled to the demux) and configured to assist the respective processor in performing security operations on the portion of the data (paragraph 0037, lines 1-20), *wherein the crypto-units (cryptographic processors) are used to help carry out the cryptographic*

Art Unit: 2131

*operations.*

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Blaker discloses:

The system of claim 1, wherein each of the plurality of processors comprises:

logic configured to identify a security association related to the portion of the data (paragraph 0042, lines 9-13), *wherein an IPSec SPI is evaluated;*

logic configured to filter the portion of the data based on the identified security association (paragraph 0042, lines 7-18), *wherein the packets are placed in an order depending on the type of packet;*

logic configured to divide the portion of the data into fragments and to reassemble the fragments into the portion (paragraph 0044, lines 1-5), *wherein data is broken up into related packets; and*

logic configured to identify a sequence associated with the portion of the data (paragraph 9, lines 8-15), *wherein a sequence identifier is assigned to each packet which determines the order of related packets.*

Claim 6 is rejected as applied above in rejecting claim 1. Furthermore, Blaker discloses:

The system of claim 1, wherein each of the plurality of processors is further configured to perform, in parallel to one another, quality-of-service (QoS) operations on the portion of the data in coordination with performing the security operations

Art Unit: 2131

(paragraph 0009, lines 16-18, paragraph 0015, lines 3-7), *wherein packets are ordered based on classification.*

Claim 7 is rejected as applied above in rejecting claim 6. Furthermore, Blaker discloses:

The system of claim 6, wherein each of the plurality of processors comprises:  
logic configured to identify an information flow associated with the data  
(paragraph 0010, lines 1-9), *wherein flow identifiers are assigned to related packets;*  
logic configured to determine a priority of the information flow (paragraph 0015, lines 1-7), *wherein the output of the parallel processors can be controlled based on the flow identifier, and*  
logic configured to manage the transfer of data into and out of the memory based on the priority of the information flow associated with the data (paragraph 0015, lines 1-7), *wherein the output of the parallel processors can be controlled based on the flow identifier.*

Claim 8 is rejected as applied above in rejecting claim 7. Furthermore, Blaker discloses:

The system of claim 7, comprising at least one of:  
an enqueue coprocessor coupled to the plurality of processors and to the data coprocessor, the enqueue coprocessor configured to manage the information flow associated with the data external to the system (paragraph 0039, lines 1-12), *wherein*

Art Unit: 2131

*related packets are classified in a flow and are classified as either inbound or outbound packets;*

a policy coprocessor configured to assist the plurality of processors in managing the transfer of the data into and out of the memory by enforcing policies of the information flow associated with the data (paragraph 0057, lines 1-12), *wherein an output admission policy is used to output packets;* and

a counter coprocessor configured to provide statistics related to the transfer of the data into and out of the memory and the enforcing of policies of the information flow (paragraph 0015, lines 1-7), *wherein the output of the parallel processors can be controlled based on the flow identifier.*

Claim 9 is rejected as applied above in rejecting claim 1. Furthermore, Blaker discloses:

The system of claim 1, wherein each of the plurality of processors is configured to execute programmable instructions for performing the security operations on the portion of the data from a plurality of independent instruction streams, and can switch between instruction streams in a single clock cycle (paragraph 0037, lines 1-7), *wherein the packets are subject to encryption, decryption, and functions associated with IPSec or SSL packets.*

Claim 10 is rejected as applied above in rejecting claim 9. Furthermore, Blaker discloses:

Art Unit: 2131

The system of claim 9, wherein each of the plurality of security processors includes separate queues corresponding to each of the independent instruction streams (paragraph 0059, lines 1-4), *wherein each crypto-unit has its own output buffer (queue).*

Claim 11 is rejected as applied above in rejecting claim 1. Furthermore, Blaker discloses:

The system of claim 1, wherein each of the plurality of processors comprises:  
logic configured to compress the portion of the data prior to performing the security operations when the portion is non-secure data (paragraph 0037, lines 27-36), *compression processor* ; and

logic configured to decompress the portion of the data after performing the security operations when the portion is secure data (paragraph 0037, lines 27-36), *compression processor*.

Claim 12 is rejected as applied above in rejecting claim 11. Furthermore, Blaker discloses:

The system of claim 11, wherein each security processor is configured to assist the respective processor in compressing and decompressing the portion of the data (paragraph 0037, lines 27-36), *compression processor*.

Regarding claim 13, Blaker discloses:



A method for performing security operations on network data, the method comprising:

transferring data into memory (paragraph 0042, lines 1-7: *crypto-input demux and crypto-output demux*);

performing security operations on respective portions of the data in parallel using a plurality of processors (paragraph 0037, lines 12-23, paragraph 45, lines 5-7: *plurality of cryptographic processors in parallel*);

using a plurality of security coprocessors to assist in performing the security operations on the respective portions of the data, each security coprocessor being coupled to a respective one of the processors (paragraph 0037, lines 1-20), *wherein the crypto-units (cryptographic processors) are used to help carry out the cryptographic operations*; and

transferring the operated-on portions of the data out of the memory (paragraph 0042, lines 1-7: *crypto-input demux and crypto-output demux*).

Claim 14 is rejected as applied above in rejecting claim 13. Furthermore, Blaker discloses:

The method of claim 13, wherein the security operations performed by each of the processors comprise:

identifying a security association related to a portion of the data (paragraph 0042, lines 9-13), *wherein an IPSec SPI is evaluated*;

Art Unit: 2131

filtering the portion of the data based on the identified security association (paragraph 0042, lines 7-18), *wherein the packets are placed in an order depending on the type of packet;*

dividing the portion of the data into fragments (paragraph 0044, lines 1-5), *wherein data is broken up into related packet;*

reassembling the fragments into the portion of data (paragraph 0044, lines 1-5);  
and

identifying a sequence associated with the portion of the data (paragraph 9, lines 8-15), *wherein a sequence identifier is assigned to each packet which determines the order of related packets.*

Claim 17 is rejected as applied above in rejecting claim 13. Furthermore, Blaker discloses:

The method of claim 13, comprising:

performing quality-of-service (QoS) operations on the respective portions of the data in parallel using the plurality of processors in coordination with performing the security operations (paragraph 0009, lines 16-18, paragraph 0015, lines 3-7), *wherein packets are ordered based on classification.*

Claim 18 is rejected as applied above in rejecting claim 17. Furthermore, Blaker discloses:

The method of claim 17, wherein the QoS operations performed by each of the processors comprise:

identifying an information flow associated with the data (paragraph 0010, lines 1-9), *wherein flow identifiers are assigned to related packets;*

determining a priority of the information flow (paragraph 0015, lines 1-7), *wherein the output of the parallel processors can be controlled based on the flow identifier, and*

managing the transfer of data into and out of the memory based on the priority of the information flow associated with the data (paragraph 0015, lines 1-7), *wherein the output of the parallel processors can be controlled based on the flow identifier.*

Claim 19 is rejected as applied above in rejecting claim 18. Furthermore, Blaker discloses:

The method of claim 18, comprising:

managing the information flow after transferring the operated-on portions of the data associated with the information flow out of the memory (paragraph 0039, lines 1-12), *wherein related packets are classified in a flow and are classified as either inbound or outbound packets;*

enforcing policies of the information flow associated with the data (paragraph 0057, lines 1-12), *wherein an output admission policy is used to output packets; and*

providing statistics related to the transfer of the data into and out of the memory and the enforcing of policies of the information flow (paragraph 0015, lines 1-7), *wherein the output of the parallel processors can be controlled based on the flow identifier.*

Claim 20 is rejected as applied above in rejecting claim 13. Furthermore, Blaker discloses:

The method of claim 13, comprising:

compressing the respective portions of the data prior to performing the security operations when the portions are non-secure data (paragraph 0037, lines 27-36),  
*compression processor*, and

decompressing the respective portions of the data after performing the security operations when the portions are secure data (paragraph 0037, lines 27-36),  
*compression processor*.

Claim 21 is rejected as applied above in rejecting claim 13. Furthermore, Blaker discloses:

The method of claim 13, comprising:

using each security processor to assist the respective processor in compressing and decompressing the portions of the data (paragraph 0037, lines 27-36), *compression processor*.

Regarding claim 22, Blaker discloses:

A computer readable medium containing a computer program for performing security operations on network data, wherein the computer program comprises executable instructions for:

transferring data into memory (paragraph 0042, lines 1-7: *crypto-input demux and crypto-output demux*);

performing security operations on respective portions of the data in parallel using a plurality of processors (paragraph 0037, lines 12-23, paragraph 45, lines 5-7: *plurality of cryptographic processors in parallel*);

using a plurality of security coprocessors to assist in performing the security operations on the respective portions of the data, each security coprocessor being coupled to a respective one of the processors (paragraph 0037, lines 1-20), *wherein the crypto-units (cryptographic processors) are used to help carry out the cryptographic operations*; and

transferring the operated-on portions of the data out of the memory (paragraph 0042, lines 1-7: *crypto-input demux and crypto-output demux*).

Claim 23 is rejected as applied above in rejecting claim 22. Furthermore, Blaker discloses:

The computer readable medium of claim 22, wherein the instructions for performing security operations on respective portions of the data in parallel using a plurality of processors comprise executable instructions for:

identifying a security association related to a portion of the data (paragraph 0042, lines 9-13), *wherein an IPSec SPI is evaluated*;

filtering the portion of the data based on the identified security association (paragraph 0042, lines 7-18), *wherein the packets are placed in an order depending on the type of packet;*

dividing the portion of the data into fragments (paragraph 0044, lines 1-5), *wherein data is broken up into related packet;*

reassembling the fragments into the portion of data (paragraph 0044, lines 1-5);  
and

identifying a sequence associated with the portion of the data (paragraph 9, lines 8-15), *wherein a sequence identifier is assigned to each packet which determines the order of related packets.*

Claim 26 is rejected as applied above in rejecting claim 22. Furthermore, Blaker discloses:

The computer readable medium of claim 22, wherein the computer program comprises executable instructions for:

performing quality-of-service (QoS) operations on the respective portions of the data in parallel using the plurality of processors in coordination with performing the security operations (paragraph 0009, lines 16-18, paragraph 0015, lines 3-7), *wherein packets are ordered based on classification.*

Claim 27 is rejected as applied above in rejecting claim 26. Furthermore, Blaker discloses:

The computer readable medium of claim 26, wherein the instructions for performing QoS operations on the respective portions of the data in parallel using the plurality of processors in coordination with performing the security operations comprise executable instructions for:

identifying an information flow associated with the data (paragraph 0010, lines 1-9), *wherein flow identifiers are assigned to related packets;*

determining a priority of the information flow (paragraph 0015, lines 1-7), *wherein the output of the parallel processors can be controlled based on the flow identifier, and*

managing the transfer of data into and out of the memory based on the priority of the information flow associated with the data (paragraph 0015, lines 1-7), *wherein the output of the parallel processors can be controlled based on the flow identifier.*

Claim 28 is rejected as applied above in rejecting claim 27. Furthermore, Blaker discloses:

The computer readable medium of claim 27, wherein the computer program comprises executable instructions for:

managing the information flow after transferring the operated-on portions of the data associated with the information flow out of the memory (paragraph 0015, lines 1-7), *wherein the output of the parallel processors can be controlled based on the flow identifier,*

enforcing policies of the information flow associated with the data (paragraph 0057, lines 1-12), *wherein an output admission policy is used to output packets; and*

Art Unit: 2131

providing statistics related to the transfer of the data into and out of the memory and the enforcing of policies of the information flow.

Claim 29 is rejected as applied above in rejecting claim 22. Furthermore, Blaker discloses:

The computer readable medium of claim 22, wherein the computer program comprises executable instructions for:

compressing the respective portions of the data prior to performing the security operations when the portions are non-secure data (paragraph 0037, lines 27-36),  
*compression processor*, and

decompressing the respective portions of the data after performing the security operations when the portions are secure data (paragraph 0037, lines 27-36),  
*compression processor*.

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.



Claims 3-5, 15-16, and 24-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Blaker et al. (U.S. Patent Pub. No. US 2003/0081600 A1) in view of Grohoski et al. (U.S. Patent Pub. No. US 2004/0225885 A1).

Claim 3, 15 and 24 are rejected as applied above in rejecting claims 1, 13, and 22, respectively. Furthermore, Blaker discloses:

logic configured to establish a security association related to the portion of the data, wherein the security association includes information used to obscure and decipher the portion and to determine the integrity of the portion (paragraph 0037, lines 1-7), wherein the packets can be subject to encrypting and decrypting per IPsec (security associations) or SSL.

Blaker does not explicitly disclose that there is logic to obscure or decipher a portion of the data depending on if the data is secure or non-secure. Grohoski discloses a system wherein a cryptographic co-processor and a CPU (external memory) communicate to process packets and subject the packet to encryption (obscure) or decryption (decipher) using information from a control word and whether the received packet was encrypted or decrypted (Grohoski: paragraph 0058, line 6 – paragraph 0060, line 4). Blaker and Grohoski are analogous arts as both use cryptographic co-processors to assist with the cryptographic processing of packets. Blaker already possesses the capability of identifying what type of packet is received (Blaker: paragraph 0037, lines 1-4) and it would have been obvious to use the control words to encrypt or decrypt the packet

based on the type of packet is received. It would have been obvious to use the method of Grohoski in combination with Blaker so that the "one or more crypto units that are optimized to perform a selected encryption process" (Grohoski: paragraph 0022, lines 3-8).

Claims 4, 16, and 25 are rejected as applied above in rejecting claim 1, 13, and 22, respectively. Blaker does not explicitly disclose a search engine coprocessor coupled to the memory and to the plurality of processors, the search engine coprocessor being configured to exchange control information between at least one of the memory and external system memory and each of the plurality of processors for use in performing security operations on the data. Grohoski discloses a system wherein a cryptographic co-processor and a CPU (external memory) communicate to process packets and subject the packet to encryption (obscure) or decryption (decipher) using information from a control word and whether the received packet was encrypted or decrypted (Grohoski: paragraph 0058, line 6 – paragraph 0060, line 4). Blaker and Grohoski are analogous arts as both use cryptographic co-processors to assist with the cryptographic processing of packets. Blaker already possesses the capability of identifying what type of packet is received (Blaker: paragraph 0037, lines 1-4) and it would have been obvious to use the control words to encrypt or decrypt the packet based on the type of packet is received. It would have been obvious to use the method of Grohoski in combination with Blaker so that the "one or more crypto units that are optimized to perform a selected encryption process" (Grohoski: paragraph 0022, lines 3-8).

Claim 5 is rejected as applied above in rejecting claim 4. Furthermore, Blaker discloses:

The system of claim 4, comprising: a memory coprocessor coupled to the plurality of processors, the memory, and the external system memory, the memory coprocessor configured to determine a status of the memory and the external system memory (paragraph 0040, lines 1-13), *wherein the capacity of the queues in the crypto units are used so that packets are queued using a fairness scheme.*

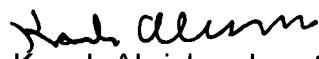
### ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2131

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

  
Kaveh Abrishamkar 10/15/07  
AU 2131

KA  
10/15/07